Bundesversicherungsamt

Bundesversicherungsamt, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Sozialversicherungsträger

- per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1951
FAX +49 228 619 1872

referat_116@bvamt.bund.de
www.bundesversicherungsamt.de

BEARBEITER(IN) Corinna Hudec

22. Mai 2018

AZ 116-8241--2075/2017
(bei Antwort bitte angeben)

nachrichtlich:
Bundesministerium für Arbeit und Soziales, Referat IV a 1
Bundesministerium für Gesundheit, Referat 211
Ministerien und Senatsverwaltung für Gesundheit und Soziales der Länder
Bundesbeauftragte für den Datenschutz und die Informationssicherheit, Referat 13
Verband der Ersatzkassen e. V., Datenschutzbeauftragte
GKV-Spitzenverband, Stabsbereich Justiziariat

Datenverarbeitung und Datenschutz – Umsetzung der EU-Datenschutzgrundverordnung; Einführung eines Datenschutzmanagementsystems (DSMS)

Sehr geehrte Damen und Herren,

ab dem 25. Mai 2018 findet die neue EU-Datenschutzgrundverordnung (im Folgenden kurz: DSGVO) nach einer zweijährigen Umstellungsphase Anwendung. Gleichzeitig treten einige, bereits auf die DSGVO abgestellte, spezialrechtliche Vorschriften in Kraft, unter anderem auch Teile des Sozialgesetzbuchs (kurz: SGB).

Das Bundesversicherungsamt unterstützt die bundesunmittelbaren Sozialversicherungsträger in dieser Umstellungsphase durch verschiedene Hilfestellungen. Neben den vielfältigen Beratungen in Einzelfragen führen wir eine sog. FAQ-Liste, in der wir die häufig diskutierten Fragen und unsere Einschätzungen hierzu dokumentieren. Zudem haben wir auf unserer

Internetseite Mustervordrucke für die Anzeige von Aufragsverarbeitungen (§ 80 SGB X i.V.m. Artikel 28 DSGVO) und die Meldung von Verletzungen des Schutzes personenbezogener Daten (§ 83a SGB X i.V.m. Artikel 33 DSGVO) angeboten, um einen vollständigen und strukturierten Austausch mit uns als Rechtsaufsicht zu erreichen.

Mit diesem Schreiben knüpfen wir an die bisherigen Hilfestellungen an. Ziel ist es, einen Ordnungsrahmen für die durch die DSGVO erforderlichen Änderungen aus Sicht eines organisationsweiten Managementsystems vorzuschlagen, der zugleich den Umfang und die Strukturierung in Zukunft geplanter Prüfungen auf diesem Gebiet transparent machen soll.

Ausgangslage:

Es ist mittlerweile weitestgehend unstrittig, dass sich die Umsetzung der DSGVO nicht auf die Einführung einzelner Datenschutzinstrumente begrenzt. Auch wird ein Nachjustieren vorhandener Regelungen kaum zu einer Gewährleistung des nunmehr EU-weiten geltenden Rechtsrahmens führen. Vielmehr erfordern die normierten Grundsätze – allen voran die Rechenschaftspflichten der Verantwortlichen (engl. *Accountability*; Artikel 5 Absatz 2 DSGVO) – einen aus Organisationssicht ganzheitlichen Ansatz. Im Ergebnis müssen die jeweils Verantwortlichen nachweisen, dass sie angemessene und wirksame Maßnahmen ergriffen haben, um die datenschutzrechtlichen Grundsätze (insb. Artikel 5 DSGVO) und Verpflichtungen (z. B. Artikel 13 ff. DSGVO) zu gewährleisten.

Ebenfalls ist unbestritten, dass die zunehmend komplexen datenschutzrechtlichen Anforderungen effektiv und effizient erfüllt werden können, wenn die korrespondierenden Aufgaben in die Geschäftsprozesse der Organisation integriert bzw. dort verankert werden. Dies führt zu dem Schluss, dass auch das Datenschutzmanagement nach den Maßstäben anerkannter Managementstandards zu einem integrierten System ausgebaut werden kann und sollte (vgl. u. a. https://de.wikipedia.org/wiki/Datenschutzmanagement, Zugriff: 8. Mai 2018).

Vor diesem Hintergrund definieren wir ein **Datenschutzmanagementsystem** (im Folgenden kurz: DSMS) als Gesamtheit der miteinander verbundenen und abgestimmten Elemente (Strukturen, Aufgaben, Prozesse, Methoden, Instrumente etc.), die erforderlich sind, um als Unternehmen oder Behörde den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Im Folgenden spannen wir hierfür einen möglichen Bezugsrahmen auf und ordnen wesentliche datenschutzrechtliche Anforderungen zu den jeweiligen Gestaltungsbereichen. Eine organisationsspezifische Ausgestaltung kann als DSMS bezeichnet werden.

Gestaltungsrahmen für ein DSMS:

1	**Organisation und Verantwortung**
1.1	Definition des Verantwortlichen im Sinne der DSGVO (Artikel 4 Nr. 7 DSGVO) und Benennung des für die Verarbeitung Verantwortlichen (Artikel 24 DSGVO).
1.2	Benennung einer/eines behördlichen Datenschutzbeauftragten (Artikel 37 DSGVO).
1.3	Verdeutlichung der Aufgaben und Aufgabengrenzen der bzw. des Datenschutzbeauftragten (Artikel 39 DSGVO).
1.4	Verpflichtung auf das Datengeheimnis und Schulungen der eigenen Mitarbeiter (Artikel 39 Absatz 1 DSGVO).
1.5	Einrichtung von Prozessen und Definition von Verantwortlichen für die Durchführung von Haftungs- und Schadenersatzverfahren (Artikel 82) sowie Verfahren zu Geldbußen und Sanktionen der Datenschutzaufsichtsbehörden (Artikel 83 und 84 DSGVO).
1.6	Erstellung verbindlicher interner Datenschutzvorschriften (Artikel 4 Nr. 20 DSGVO), in der auch die wesentlichen organisatorischen Verantwortlichkeiten geregelt sind.
2	**Gewährleistung allgemeiner Pflichten des Verantwortlichen**
2.1	Einrichtung eines risikoorientierten Entscheidungsprozesses, um geeignete technische und organisatorische Maßnahmen für eine datenschutzkonforme Verarbeitung umzusetzen und diese regelmäßig auf Aktualität und Wirksamkeit zu überprüfen, insbesondere was den Stand der Technik anbelangt. In der Sekundärliteratur wird in diesem Kontext oftmals die Einrichtung eines sog. Plan-Do-Check-Act-Zyklus verwiesen, der eine kontinuierliche Überwachung nach dem Regelkreisprinzip vorsieht (Artikel 24 i. V. m. Artikel 32 DSGVO).
2.2	Einrichtung von (Teil-)Prozessen, die im Rahmen der originären Beschaffungs- und Entwicklungsprozesse eine datenschutzfreundliche Technikgestaltung (engl. *Data Privacy by Design*) und datenschutzfreundliche Voreinstellungen (engl. *Data Privacy by Default*) gewährleisten (Artikel 25 DSGVO).
2.3	Erarbeitung und Umsetzung eines organisationsweiten Löschkonzepts zur Wahrung des Grundsatzes der Datenminimierung (Artikel 5 Absatz 1 Bst. c) DSGVO), z. B. nach den Vorgaben der „Leitlinie zur Entwicklung eines Löschkonzepts mit der Ableitung von Löschfristen für personenbezogene Daten“ (vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/ Leitlinie_zur_ Entwicklung_eines_Loeschkonzepts.html, letzter Zugriff: 11. Mai 2018).
3	**Maßnahmen zur Wahrung der Betroffenenrechte**
3.1	Einrichtung eines Prozesses, um die Auskunftsrechte der betroffenen Personen in der definierten inhaltlichen Ausprägung in einer angemessenen Frist sicherzustellen (Artikel 15 DSGVO).
3.2	Einrichtung von Prozessen und Einsatz von geeigneten technischen Hilfsmitteln, um das Recht auf Berichtigung (Artikel 16 DSGVO), das Recht auf Löschung (Artikel 17 DSGVO) und das Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO) zu gewährleisten.

3.3	Einrichtung eines Prozesses zur Benachrichtigung von Empfängern personenbezogener Daten, soweit diese berichtigt, gelöscht oder deren Verarbeitung eingeschränkt wurde (Artikel 19 DSGVO).
3.4	Einrichtung von Prozessen und technischen Möglichkeiten zur sog. Datenportabilität (Recht auf Datenübertragbarkeit – Artikel 20 DSGVO).
3.5	Einrichtung von Prozessen zur Berücksichtigung des Widerspruchsrechts (Artikel 21 DSGVO).
3.6	Identifikation von ausschließlich automatisierten Verarbeitungsvorgängen, zu denen besondere Maßnahmen zu treffen sind, insbesondere die Eröffnung der Möglichkeit, die automatisierte Entscheidung anfechten zu können (Artikel 22 Absatz 3 DSGVO).
4	**Sicherstellung der Informationspflichten gegenüber den Betroffenen**
4.1	Identifikation der relevanten Informationspflichten im Zusammenhang mit der Erhebung personenbezogener Daten (Artikel 13 DSGVO) sowie Informationspflichten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Artikel 14 DSGVO) und Auswahl geeigneter Informationsmittel.
4.2	Einrichtung eines Prozesses zur kontinuierlichen Aktualisierung der Informationspflichten zu Punkt 4.1.
5	**Verzeichnis für Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung**
5.1	Festlegung eines geeigneten Formats für ein Verarbeitungsverzeichnis (Artikel 30 DSGVO) als zentrales Instrument zur Umsetzung der Nachweispflicht (Artikel 5 Absatz 2 DSGVO).
5.2	Einrichtung geeigneter Prozesse, um das Verarbeitungsverzeichnis inhaltlich aufzustellen und zu aktualisieren (siehe hierzu auch Anmerkungen zu Punkt 2.1).
5.3	Etablierung eines Prozesses zur Datenschutz-Folgeabschätzung, soweit von einer Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen ausgeht (Artikel 35 DSGVO).
5.4	Konsultation mit der Datenschutzaufsichtsbehörde, falls keine Maßnahmen zur Eindämmung eines hohen Risikos getroffen werden können (Artikel 36 DSGVO).
6	**Einrichtung eines Vertragsmanagements zum Datenschutz**
6.1	Einrichtung eines Prozesses für die Vereinbarung von verschiedenen Verschwiegenheitsverpflichtungen.
6.2	Neugestaltung von Einwilligungserklärungen und Abstimmung organisationsweiter Regeln zur Form und Dokumentation in den Fachprozessen (Artikel 7 DSGVO).
6.3	Einrichtung eines Prozesses zur Ausgestaltung individueller Vereinbarungen zur Auftragsverarbeitung (kurz: AVV - Artikel 28 DSGVO), insb. Festlegung der zu beteiligenden Stellen.
6.4	Vereinbarungen zur gemeinsamen Verantwortung (engl. *Joint Controllership*) gemäß Artikel 26 DSGVO.

7	Umgang mit Datenschutzverletzungen
7.1	Einrichtung von Prozessen zur Dokumentation und zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzaufsichtsbehörden (Artikel 33 DSGVO) und die Rechts- oder Fachaufsichtsbehörde (§ 83a SGB X).
7.2	Strukturierte und vollständige Erfassung der meldungsrelevanten Aspekte z. B. durch die Verwendung von Mustervordrucken (vgl. https://www.bundesversicherungsamt.de/aufsicht/datenverarbeitungdatenschutz.html, letzter Zugriff: 11. Mai 2018).
7.3	Einrichtung eines Prozesses zur Benachrichtigung der von einer Verletzung betroffenen Person (Artikel 34 DSGVO).
7.4	Berücksichtigung von Erkenntnissen aus der Analyse der Datenschutzverletzungen im Rahmen der kontinuierlichen Überprüfung der Schutzmaßnahmen (z. B. Initiierung eines PDCA-Zyklus, siehe Punkt 2.1)

Erläuterungen:

Mit der (etwas verkürzten) Formulierung „Einrichtung von Prozessen" ist die Definition, Modellierung und Dokumentation von **Geschäftsprozessen** gemeint. Diese umfassen ein definiertes Ereignis, durch das eine Menge logisch verknüpfter Aktivitäten ausgelöst werden und auf ein bestimmtes Ergebnis ausgerichtet sind. Im Idealfall sind die Geschäftsprozesse zum Datenschutzmanagement in das organisationsweite Geschäftsprozessmodell integriert. Die Dokumentation sollte ebenfalls einheitlich modelliert sein.

Die Dokumentationspflicht eines solchen Datenschutzmanagementsystems ergibt sich aus der in Artikel 5 Absatz 2 DSGVO verankerten Rechenschaftspflicht. Nach unserer Auffassung ist eine unternehmens- bzw. behördenindividuelle **Datenschutzrichtlinie** das richtige Format hierfür. Die Richtlinie sollte auf Managementebene einen Überblick über die Regelungsbereiche bieten und ggf. detailliertere Dokumentationen einzelner Verfahren verweisen (vgl. u. a. Jung, Alexander: Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO. In: ZD 2018, 208, Seite 211).

Der herausgearbeitete Ordnungsrahmen ist unverbindlich. Jede andere Strukturierung kann ebenfalls geeignet sein, die Dokumentations- und Rechenschaftspflichten zu erfüllen. Wir erheben auch keinen Anspruch auf Vollständigkeit der jeweils als Prozess umzusetzenden gesetzlichen Anforderungen.

Ausblick:

Das Bundesversicherungsamt wird zukünftig entlang des oben dargestellten Ordnungsrahmens die datenschutzrechtlichen Anforderungen stichprobenartig prüfen. Die Einrichtung eines Datenschutzmanagementsystems und die Vorlage einer übergreifenden Dokumentation können in diesem Kontext ein hilfreicher Ausgangspunkt der Prüfung sein.

Für Rückfragen und Diskussionen zu diesem Rundschreiben stehen wir Ihnen unter den bekannten Kontaktmöglichkeiten gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)